WORLD **PRIVACY** FORUM

Comments of the World Privacy Forum
to the President's Identity Theft Task Force
Regarding September 19, 2006 Interim Recommendations

January 18, 2006

VIA email to Taskforcecomments@idtheft.gov

Pursuant to a request for comments published by the President's Identity Theft Task Force,[1] the World Privacy Forum respectfully submits these comments regarding the September 19, 2006 Interim Recommendations of the President's Identity Theft Task Force. The World Privacy Forum is a non-profit public interest research group that focuses on in-depth analysis and research of privacy topics, including identity theft.[2]

Our comments discuss concerns in two areas: first, the exclusion of medical identity theft from the interim recommendations, and second, Privacy Act issues with the recommended data breach language.

I. Introduction

We are pleased the Task Force is looking for ways to close gaps in protections for victims of identity theft, among other tasks. But the omission of medical identity theft from the interim recommendations is an oversight that needs to be addressed. It is our hope that our comments will shed light on the reasons why this oversight needs to be remedied.

Medical identity theft[3] is a crime that has the following characteristics:

---

[1] < http://www.ftc.gov/opa/2006/12/fyi0688.htm >. The solicitation for comments was published December 26, 2006.

[2] <http://www.worldprivacyforum.org>.

[3] The World Privacy Forum defines medical identity theft as follows: "Medical identity theft occurs when someone uses a person's name and sometimes other parts of their identity – such as insurance information -- without the person's knowledge or consent to obtain medical services or goods, or uses the person's identity information to make false claims for medical services or goods. Medical identity theft frequently results in erroneous entries being put into existing medical records, and can involve the creation of fictitious medical records in the victim's name" (Dixon, Pam; Gellman, Robert. *Medical Identity Theft: The Information Crime That Can Kill You*, World Privacy Forum, May 2006, p.5. <http://www.worldprivacyforum.org/pdf/wpf_medicalidtheft2006.pdf>.

1. Medical identity theft exists; this is an unambiguous fact. This crime is distinct in its operation, types of harm, and victim recourse; as such, it differs from purely financial forms of the crime. Medical identity theft typically leaves a trail of falsified information in medical records that can plague victims' medical and financial lives for years. For documentation and discussion of the facts, processes, and dimensions of this crime, we refer you to our May 2006 report on medical identity theft (*Medical Identity Theft: The Information Crime That Can Kill You*, http://www.worldprivacyforum.org/pdf/wpf_medicalidtheft2006.pdf), as well as to our FAQ and consumer education materials on this crime http://www.worldprivacyforum.org/medicalidentitytheft.html.

2. Medical identity theft harms its victims in substantive ways ranging from potential financial impacts (like financial identity theft victims) to health impacts (changes to medical files that have the potential for impacts on health and treatment decisions), as well as decisions about future employment or insurance coverage, and more.

3. Medical identity theft has not yet been clearly addressed by federal agencies.

4. Medical identity theft victims do not enjoy the same recourse, education, help, or recovery support that victims of purely financial forms of the crime receive from federal agencies. In short, victims of medical identity theft do not have a clear place to turn to for help within the federal government, nor do they have a clear recovery pathway.

We believe it is not anyone's fault that medical identity theft victims have not received the help they need to date, but since this group of victims is now known to be in existence and to have special needs for assistance with recovery, the World Privacy Forum would like to focus the Task Force on these victims with the idea that the Task Force can help smooth the inter-agency cooperation that will be needed to help them.

II. Removing obstacles to victim recovery: Gaps that exist for medical identity theft victims need to be considered and resolved

There is a disparity between the experience of victims of financial forms of identity theft and medical forms of identity theft. Disparities of rights and educational support afforded to victims have contributed to the challenging, and sometimes impossible to overcome, obstacles for victims of medical identity theft.

The primary challenges medical identity theft victims face include:

- Lack of enforceable rights to correct medical records in all instances of occurrence; lack of enforceable rights to delete information put in records as a side effect or as a direct result of fraudulent activities.

- Lack of a government agency designated to help victims of medical forms of identity theft.

- Lack of ability in most cases to find all instances of medical records. (Records at insurance companies, labs, medical groups, and so on.)

- Lack of resources focused on the specific educational, informational, and recovery assistance needs of medical identity theft victims.

We observe that some of these issues, such as lack of enforceable rights in areas related to victim recovery, are recalcitrant and could take years to resolve. But we also observe that other issues, such as providing educational resources at the federal level about medical identity theft, and designating a federal agency for victim assistance and education, could be accomplished more quickly.

Disparity of Enforceable Rights

Victims of financial identity theft can depend on rights such as the ability to see and correct errors in their credit report, the ability to file fraud alerts, the right to obtain documents or information relating to transactions involving their personal information, and the right to prevent consumer reporting agencies (such as credit bureaus) from reporting information that has resulted from of identity theft.[4]

But victims of medical identity theft do not have a similar complete set of rights or redresses. Victims of medical identity theft do not have the blanket right to correct errors in their medical files. In some cases, victims have not been allowed to even see the compromised files. And victims of medical identity theft do not have the right to prevent health care providers, medical clearinghouses, or insurers from reporting and re-reporting information that has resulted from identity theft. These disparities in rights should be looked at by the Task Force.

Disparity of Educational Support

Another disparity victims of medical identity theft face relates to a lack of educational support. The FTC is doing an excellent job providing education to financial identity theft victims about their rights and supporting them through the recovery process. But the high-quality tips and resources afforded to victims of financial forms of identity theft do not extend to the medical and insurance aspects of identity theft crimes. As a result, victims of medical identity theft may generally experience multiple difficulties in attempting to recover, and may also be unable to find adequate information to get help.

---

[4] The FTC has a detailed page describing these rights and specific actions to take: Take Charge: Fighting Back Against Identity Theft. <http://www.ftc.gov/bcp/conline/pubs/credit/idtheft.htm>. See also Government Accountability Office, , Identity Theft Rights: Some Outreach Efforts to Promote Awareness of New Consumer Rights are Underway, (June 2005) (GAO-05-710).

Financial identity theft recovery information alone cannot always resolve all of the issues medical identity theft victims face. In some cases, victims of medical identity theft may need specific HIPAA-related questions answered, as well as needing financial identity theft information.

The advice that is often given to victims of financial identity theft is not sufficient to help them to recover, and needs to be augmented with **specific recommendations for victims of medical identity theft**. This may sound seemingly simple to accomplish, but at the federal level the reality is that these recommendations immediately become a complex matter because medical identity victims generally cross over between financial recovery and recovery related directly to HIPAA issues (such as accounting of disclosures, HIPAA appeals for access to victim records, and so forth).

Closing the Gaps

The gaps in current levels of consumer education and government support in the area of medical identity theft have been inadvertent and unintentional. The Federal Trade Commission (FTC), which has studied financial identity theft, boasts robust financial identity theft resources, but is not responsible for addressing medical issues or answering questions about correcting files and records under HIPAA. That falls to the Department of Health and Human Services. DHHS has not published focused studies or guidance about medical identity theft, and does not have the same levels of financial identity theft expertise that the FTC does, as that falls to the FTC.

The World Privacy Forum has created a FAQ specifically for medical identity theft victims. The FAQ includes sample letters and information for victims that maps out specific steps to recovery. This is an important beginning, but for the most robust support possible, it will be important for victims to have federal informational resources and support available to them.

However, which agency will accomplish this? This FTC, with its expertise in financial forms of identity theft, or DHHS, which has expertise in HIPAA? This is something the Task Force needs to analyze and resolve. Can there be a "one-stop shop" for these victims? We have hopes that the joint Task Force is exactly the kind of vehicle that can facilitate exploration of this question and enable a speedy resolution.

The Executive Order that created the Task Force states one of the goals of the Task Force is:

> (b) improved public outreach by the Federal Government to better (i) educate the public about identity theft and protective measures against identity theft...[5]

Again, we reiterate the point that while some disparities will take many years to resolve,

[5] Executive Order, *Strengthening Federal Efforts To Protect Against Identity Theft*, May 10, 2006. < http://www.whitehouse.gov/news/releases/2006/05/20060510-3.html >.

providing educational support and designating the right agency or agencies for medical identity theft victims to go to for help can be accomplished much more quickly, and could go far in helping remove obstacles for these victims. We urge and encourage the Task Force to take on this job, which if effectively completed, could help so many individuals.

III. Data Breach Notice and Routine Use: Privacy Act issues with the interim draft language

The Task Force has recommended that federal agencies publish a routine use that specifically permits the disclosure of information in connection with response and remedial efforts in the event of a data breach. The Task Force suggests that agencies use as a model a recent routine use proposed by the Department of Justice (DOJ).

The World Privacy Forum believes the broad purpose of this recommendation is reasonable, but we find that there are shortcomings and consequences to the routine use proposed by the DOJ. We recommend that the Task Force rethink and narrow its recommendation to take into consideration the consequences and cost of its recommendation. A clearer, narrower, and more targeted routine use will allow the purpose to be served with less expense and disruption to unrelated activities. More importantly, a better routine use will evade the possibility of being thrown out by a court. Disclosures made under an improper routine use could expose the government to significant damages.

First, we found it difficult to evaluate the proposed DOJ routine use because of the lack of sufficient justification in the published notice. The publication contains only a single paragraph of explanation for applying a routine use to dozens of different systems of records containing substantially different types of records. We note that the broad application of the routine use to all agency systems of records will include systems that contain classified information, data on protected witnesses, employment information on covert agents, information protected by law from disclosure, and other sensitive information. We doubt that the application of a breach routine use would be appropriate or legal for all systems of records.

Any disclosure necessary for a law enforcement investigation or prosecution of a security breach is already covered by the Privacy Act itself or by existing routine uses already adopted by agencies for most systems of records. If there is a need to share information with contractors hired by an agency to ameliorate the harm from a data breach, existing routine uses covering contractor disclosures should be adequate. A common routine use for many Privacy Act systems covers disclosure to “contractors, experts, and consultants when necessary to accomplish an agency function related to a system of records.” For any additional disclosures that may be appropriate as a response to a security breach, a routine use should be specific and narrowly focused.

Second, we find the routine use too vague to meet legal standards. The proposed routine use appears to allow disclosure of any Privacy Act record to quite literally anyone in the world, and this is not intended as a glib statement. The actual text says that disclosure is permitted to "appropriate agencies, entities, and persons." The use of the modifier *appropriate* offers no meaningful limitation. A routine use that potentially allows disclosure to anyone and everyone is simply too vague to meet statutory standards for identifying the potential recipients of Privacy Act information. Indeed, the Privacy Act Overview published by the Department itself cites a case that found the use of appropriate as a qualifier to be insufficient in a routine use.[6]

An agency has an obligation to tell the public precisely what individuals and which institutions in what parts of the world might be appropriate recipients under this routine use. Would the Department of Homeland Security be a possible recipient under this routine use? Would commercial data brokers with anti-fraud products or services be a possible recipient under this routine use? Would financial sector companies such as credit bureaus be recipients under this routine use? The point is that all of these institutions and infinitely more are potential recipients under the proposed routine use as currently drafted. A routine use must be more specific and unambiguous in describing who would be eligible to receive personal information from so many different and sensitive systems of records.

The remainder of the routine use seeks to identify the purpose of the disclosure. This part too suffers from vagueness. The first clause allows disclosure when "it is suspected or confirmed that the security or confidentiality of information in the system of records has been compromised." The routine use needs to make clear precisely who has to suspect or confirm the compromise. Otherwise, speculation in the Washington Post or the suspicions of a GS-5 clerk could meet the standard. At a minimum, any "suspicions" or "confirmations" should come from a politically accountable appointee. Beyond this, there needs to be specific and detailed procedural guidelines for determining what should constitute "suspicion."

We note that the memorandum included in Appendix A to the Task Force's report observes:

> Because circumstances will differ from case to case, agencies should draw upon law enforcement expertise, including that of the agency Inspector General, in assessing the risk of identity theft from a data compromise and the likelihood that the incident is the result of or could lead to criminal activity.

---

[6] See <http://www.usdoj.gov/oip/1974condis.htm#routine>. ('In Krohn v. United States Department of Justice, No. 78-1536, slip op. at 4-7 (D.D.C. Mar. 19, 1984), however, the court invalidated an FBI routine use allowing for "dissemination [of records] during appropriate legal proceedings," finding that such a routine use was impermissibly "vague" and was "capable of being construed so broadly as to encompass all legal proceedings."').

We agree that there should be an assessment of the risk and that accountable agency personnel should make that assessment. The routine use should incorporate a requirement for an appropriate assessment and not permit disclosures based on mere suspicion.

The second clause allows disclosure when "the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information." Proving an economic or property interest under the Privacy Act of 1974 can be complex and challenging. Suppose that a different interest is affected by a security breach. A security breach might be potentially embarrassing to a data subject or cause harm to reputation. Would that type of harm permit a disclosure? It is not clear why non-economic interests of data subjects have been excluded. While we have doubts about the need for the routine use and the disclosures that it seeks to justify, we think that the second prong should not exclude the possibility of "harm to the privacy interests of data subjects."

We have an additional concern about the second clause. It allows disclosure if there is a risk of harm to the integrity of a system maintained by an "entity." It appears that the recipient of data could be a private entity (e.g., a company that maintains consumer profiles for marketing purposes) whose database may suffer harm from the security breach. If so, we question the propriety of these disclosures. When and if an agency should undertake to disclose its own Privacy Act information to a private organization to correct or update information of that organization is far from clear. If a security breach could justify information sharing with a private entity – and we concede the possibility in some narrow cases – the circumstances should be more clearly and narrowly defined. The open-ended authority of the proposed routine use is troubling.

The third clause has problems as well. It provides for disclosure when "the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm." This clause repeats the vague phrase "agencies, entities, and persons" already the subject of a previous comment. There are additional problems. Disclosures to prevent, minimize, or remedy harm seem justifiable, albeit lacking in any clear standard. However, it is not apparent what is meant by "respond to the suspected or confirmed compromise" that is not already included in preventing, minimizing, and remedying the harm. Would an attempt to hide or shift blame for a security breach qualify as a type of response? The possibility is evidence of the vagueness of the language.

If *respond* has some meaning other than preventing, minimizing, or remedying harm, the routine use should be more specific. As it stands, the routine use would allow a disclosure of all Privacy Act information to anyone in the world if some unstated person has a suspicion of a security breach, the agency determines that there is a risk of harm to some unqualified economic or property interest (regardless of the magnitude of the interest),

and the agency wants to "respond." Again, we are not being glib; this is an accurate analysis of the language as currently proposed.

Reserving the right to disclose Privacy Act records to anyone so an agency can make some unspecified "response" is just too vague to provide members of the public with the notice contemplated by Congress when it established the ability to add new disclosures via the routine use provision of the Privacy Act.

Third, we find that the notice is overbroad because it allows the disclosure of any and all records in Privacy Act systems. The routine use makes no attempt to limit the type of records that may be disclosed. If an agency has a copy of an individual's medical record (e.g., as part of a health care fraud case), the routine use allows disclosure of the entire medical record without limitation. The routine use also appears to allow the disclosure of classified information, other information restricted by law, identities of undercover agents, home addresses of agency employees, and names of confidential informants.

The categories of records that can be disclosed under the routine use should be qualified. Information that is generally restricted by law or policy should not be eligible for disclosure just because there is suspicion of a security breach, and an agency is searching for a *response*. Each federal agency has a responsibility to its employees, its informants, the subjects of incomplete investigations, and any other individuals who might be the subject of an agency file to narrow the scope of records that can be disclosed. The limits belong in the routine use itself and should not be left to the discretion of unnamed and possibly low-level employees.

Fourth, we observe that DOJ sought to add the proposed routine use to every existing system of records. However, its Federal Register notice did not explain why the routine use is necessary or appropriate for any system, let alone each system. For example, the Office of Justice Programs system 001 is an Equipment Inventory system. Is there sufficient personal information about individuals (other than title, office, telephone number) so that an unauthorized disclosure would actually give risk to a realistic concern of identity theft? A one-in-a million chance does not justify a routine use and certainly not one as broad as the proposed routine use. Where is the risk assessment for each system of records that would justify the application of a new routine use?

We believe that it would be appropriate for each agency planning to adopt a security breach routine use to prepare a detailed, system-by-system Privacy Impact Assessment for the proposed routine use. OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (M-03-22) states that "PIAs are required to be performed and updated as necessary where a system change creates new privacy risks." The addition of a routine use to all or many agency systems of record cries out for a Privacy Impact Assessment and a risk analysis. This would be true even if the proposed routine use were more narrowly written and better justified. Is the proposed routine use necessary and worth the risk entailed by the additional disclosure authority contained in the routine use? A detailed, system-by-system evaluation of risk is needed and necessary.

Addressing security breaches by advising agencies to ignore existing privacy protections and procedures is a poor tradeoff, a bad example, and a likely violation of law.

An additional problem is that the Task Force has not considered the obvious alternative to a routine use. Disclosure from a Privacy Act system of records is possible with the consent of the data subject. If a breach includes records on a relatively small number of individuals, obtaining consent is a realistic alternative. It is also a reasonable alternative. An individual who is already the subject of a suspected data breach might be just as unhappy about the disclosure of his or her record to any agency, entity, or person selected by an agency for some unspecified "response." Further disclosures made to supposedly to protect an individual might not be welcome and might only compound the problem. The Task Force should explain why consent could not be used to justify disclosure in some instances, and the bureaucratic convenience of an agency will not be a sufficient justification for every system of records.

Lastly, we observe that the addition of a new routine use to every agency system of records is likely to require a change to every agency form that collects information from an individual. Subsection (e)(3)(C) requires an individual notice on each form used to collect information of the routine uses which may be made of the information. Revising all government forms to include a new routine use is a task likely to take years and could cost millions. Further, the failure to include the information promptly on forms may make it impossible to rely on the routine use or – even worse – may make availability of the routine use inconsistent from system to system and perhaps from record to record.

We observe that if an agency relies on an existing routine use that permits disclosure to agency contractors, the principal goals of the Task Force's recommendation would be met, the ability to make disclosures under controlled circumstances to respond appropriately to security breaches would be maintained, and there would be no need to revise any forms, let alone the large number of existing forms used by federal agencies. The World Privacy Forum is not pleased with the scope of the standard contractor routine use, but it is in already in place. We would prefer to see reliance on an existing routine use rather than the promulgation of a vague and overbroad routine use applicable to many systems of records. It would be an easier, less expensive, and less troublesome alternative. If there is a need for additional disclosure authority beyond agency contractors, that authority should be much more narrowly circumscribed than in the proposed DOJ routine use.

The World Privacy Forum has no doubt that the objectives of the Task Force's recommendation on routine uses can be achieved. What is needed is the application of more Privacy Act expertise and a bit of common sense to narrow and focus the routine use so that it allows only those disclosures that will accomplish the stated purpose and so that the routine use applies only to systems of records for which it make sense. The goals of protecting privacy and reacting to security breaches will not be met through the promulgation of an unqualified routine use that allows expansive disclosures. History has shown that, however well-intentioned, authority to disclose personal information can be and will be misused.

IV. Conclusion

Thank you for inviting comments on the interim recommendations, and thank you for considering the World Privacy Forum's comments regarding medical identity theft and data breach routine uses.

Respectfully submitted,

Pam Dixon
Executive Director,
World Privacy Forum
www.worldprivacyforum.org
760.436.2489